

## FVR206 -3-Port 10/100 Firewalls

### Plug & Play Policy management Solutions for Growing Companies

With the explosive growth of the Internet, accessing information and services at any time, day or night has turned out to be a standard requirement for all enterprises. Managing enterprise network resources is an increasing challenge for many corporate network operators. The security issue is repeatedly addressed in all enterprises. To diminish the risk of exposing your network while surfing the Internet is now unquestionably a major concern for all.



The **FVR206** implements sophisticated, yet integrated solutions designed to protect and secure the integrity of network data. The **FVR206** enables organizations to utilize cost-effective public Internet transport to connect remote offices and remote users to the main corporate site, thus eliminating expensive dedicated WAN links and modem banks. Furthermore, the advent of cost-effective, high-bandwidth technologies like DSL, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth. The FVR206 find a way out to secure access as well as to enable connectivity, making the network easier to use and more secure.

#### VPN- Virtual Private Networking

- Enables corporate customers to establish secure, end-to-end, private network connections by using public-access data wires, like Internet, to connect private-user nodes.
- Use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

#### Content Filter

- URL Blocking: tracking and denying of user access to undesirable web sites based on predefined site content.
- General Blocking: blocking web pages contains applications of Cookie/Java/ActiveX/Popup likely used by hackers as Trojan horse.

#### Server Load Balancing

- Supports up to 4 virtual servers via one legal IP.
- Distributes traffic efficiently and evenly among network servers so that no individual server is overburdened. Distribute traffic evenly, skipping errant servers, and provide an additional level of fault tolerance to enhance performance, reliability, and scalability.



## SPECIFICATIONS:

General	
Network interface	Four Switch Ports (or LAN Port) One External Port (or WAN Port) One DMZ Port
Management	Firewall, VPN, Server Load Balancing, Content Filter.
CPU	Waveplus RISC
Flash Memory	8 Mbyte
SDRAM	32 MByte
Throughput	VPN mode : 1.2Mbps NO VPN mode: 12Mbps
Safety Certificate	ICSA, FCC, UL, CE, CUL, TUV

## SOFTWARE FEATURES:

Firewall	
Hacker alert	DoS auto-detect and block attacks: Ping of Death, IP Spoofing, TearDrop, PortScan, LAND, SYN...attack, block the traffic and email notification.
Connection modes	Transparent and NAT modes combined between WAN/LAN/DMZ
Network rule-Policy management	Management by object-network, user, service; defining source, destination, and service; setting rule policy by action, schedule, log and threshold.
Multi-NAT (Network Address Translation)	Permits many users on same/different subnets to share a single external IP address at the same time.
DDNS	Dynamic DNS allows customers to alias a dynamic IP address to a static hostname, so that web site can be more easily accessed by specific name though the IP address comes dynamically.
DNS Proxy	DNS Cache; bandwidth saving
Attack Alert	Real time log and email notification for hacker attack
DHCP	Supports PPPoE, DHCP Client, DHCP Server for ADSL/Cable environment
VPN (Virtual Private Network)	
Tunnels	Concurrent VPN tunnel
Algorithm	Class-base queuing; TCP Windows-sizing
VPN Gateway	Site to site IPSec; PPTP VPN Server
Server Load Balancing	
Virtual Server	Supports Socket Port Number (Virtual Server) convert
Server load Balancing	Supports up to 4 virtual servers via a legal IP address for distributing traffic evenly and efficiently.
Content Filter	
URL Blocking:	Tracks and denies user's access to undesirable web sites based on predefined site content.
General Blocking:	Blocks web pages containing Cookie/Java/ActiveX/ Popup applications which are likely used as Trojan horse by hackers.

